A simple proof of monogamy of entanglement

Dong Yang[1]

[1]Hefei National Laboratory for Physical Sciences at Microscale & Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, Peoples Republic of China

(Dated: November 3, 2006)

Monogamy of entanglement means that an entangled state cannot be shared with many parties. The more parties, the less entanglement between them. In this paper, we give a simple proof of this property and provide an upper bound of the number of parties.

PACS numbers: 03.67.Mn, 03.65.Ud

Monogamy is one of crucial properties of entanglement. It is essential in quantum cryptography. A simple example is the Bell state $|\Phi\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle$ shared between Alice and Bob. Monogamy of the pure entangled state $|\Phi\rangle_{AB}$ excludes any possibility that another party including the potential eavesdropper Eve could correlate. The monogamous property of the pure entangled state is extended to the un-sharable property for the mixed state [1, 2, 3]. In a recent paper [4], the monogamous property is employed to prove asymptotic quantum cloning is state estimation, which has been identified as one of the open problems in quantum information theory. In this paper, we give a simple proof of the monogamy of entanglement and provide an upper bound of the number of parties.

Definition 1 *A bipartite state ρ_{AB} is said to be n-sharable when it is possible to find a quantum state $\rho_{AB_1B_2\cdots B_n}$ such that $\rho_{AB_1} = \rho_{AB_2} = \cdots = \rho_{AB_n} = \rho_{AB}$ where $\rho_{AB_k} = tr_{B_{\bar{k}}}\rho_{AB_1B_2\cdots B_n}$. If such state exists, $\rho_{AB_1B_2\cdots B_n}$ is called as an n-extension of ρ_{AB}.*

Theorem 1 *[1, 2, 3] A bipartite state is n-sharable for any n if and only if it is separable.*

Proof. For a separable state ρ_{AB}, there always exists a separable decomposition

$$\rho_{AB} = \sum_i p_i(|\phi_i\rangle\langle\phi_i|)_A \otimes (|\psi_i\rangle\langle\psi_i|)_B. \tag{1}$$

It is explicit that

$$\rho_{AB_1B_2\cdots B_n} = \sum_i p_i(|\phi_i\rangle\langle\phi_i|)_A \otimes (|\psi_i\rangle\langle\psi_i|)^{\otimes n}_{B_1B_2\cdots B_n} \tag{2}$$

is a valid n-extension of ρ_{AB} for any n.

Next we prove that for any entangled state ρ_{AB}, there always exists a finite N such that no valid n-extension can be found for any $n > N$. Recall that the duality relation of a pure tripartite state ϕ_{ABC} is [5]

$$S(\rho_A) = E_f(\rho_{A:B}) + C_{\leftarrow}(\rho_{A:C}). \tag{3}$$

Here $S(\rho_A) = -tr\rho_A \log \rho_A$ is the von Neumann entropy of ρ_A. $E_f(\rho_{AB}) = \min \sum_i p_i E(\phi^i_{AB})$ is the entanglement of formation (EoF) [7], where the minimum is taken over all pure ensembles $\{p_i, |\phi^i\rangle_{AB}\}$ satisfying $\rho_{AB} = \sum_i p_i(|\phi^i\rangle\langle\phi^i|)_{AB}$, and entanglement for pure state ϕ_{AB} is $E(\phi_{AB}) = S(tr_B(|\phi\rangle\langle\phi|)_{AB})$. $C_{\leftarrow}(\rho_{A:C}) = \max_{C_i^\dagger C_i} S(\rho_A) - \sum_i p_i S(\rho^i_A)$ is the classical correlation of bipartite state ρ_{AC} [6], where $\{C_i^\dagger C_i\}$ is a positive operator-valued measurement (POVM) performed on subsystem C, $\rho^i_A = tr_C(I \otimes C_i \rho_{AC} I \otimes C_i^\dagger)/p_i$ is the remaining state of A after obtaining the outcome i on C, and $p_i = tr_{AC}(I \otimes C_i \rho_{AC} I \otimes C_i^\dagger)$ is the probability to obtain outcome i.

Suppose the optimal decomposition of EoF for a mixed tripartite state $\rho_{A:BC}$ is $\{p_i, |\phi^i\rangle_{A:BC}\}$, we have

$$\begin{aligned} E_f(\rho_{A:BC}) &= \sum p_i S(\rho^i_A) && (4)\\ &= \sum p_i (E_f(\rho^i_{A:B}) + C_{\leftarrow}(\rho^i_{A:C})) && (5)\\ &\geq E_f(\rho_{A:B}) + G_{\leftarrow}(\rho_{A:C}). && (6)\end{aligned}$$

The inequality (6) comes from the convexity of EoF $\sum p_i E_f(\rho^i_{A:B}) \geq E_f(\sum p_i \rho^i_{A:B})$ [7] and $G_{\leftarrow}(\rho_{A:C}) = \min \sum_i p_i C_{\leftarrow}(\rho^i_{A:C})$ [8], where the minimum is taken over all mixed ensembles $\{p_i, \rho^i_{AC}\}$ satisfying $\rho_{AC} = \sum_i p_i \rho^i_{AC}$.

Now iteratively applying the inequality (6) to the n-extension state $\rho_{AB_1B_2\cdots B_n}$ of an entangled state ρ_{AB} and further noticing $E_f(\rho_{A:B}) \geq G_{\leftarrow}(\rho_{A:B})$ by definition of $G_{\leftarrow}$ [8], we obtain

$$
\begin{aligned}
E_f(\rho_{A:B_1B_2\cdots B_n}) &\geq E_f(\rho_{A:B_2\cdots B_n}) + G_{\leftarrow}(\rho_{A:B_1}) \\
&\geq E_f(\rho_{A:B_3\cdots B_n}) + G_{\leftarrow}(\rho_{A:B_2}) + G_{\leftarrow}(\rho_{A:B_1}) \\
&= E_f(\rho_{A:B_3\cdots B_n}) + 2G_{\leftarrow}(\rho_{A:B}) \\
&\geq \cdots\cdots \\
&\geq E_f(\rho_{A:B}) + (n-1)G_{\leftarrow}(\rho_{A:B}) \\
&\geq nG_{\leftarrow}(\rho_{A:B}). \qquad (7)
\end{aligned}
$$

Employing the explicit relation $S(\rho_A) \geq E_f(\rho_{A:B_1B_2\cdots B_n})$ and an important property of $G_{\leftarrow}$ asserting that $G_{\leftarrow}(\rho_{A:B}) > 0$ *if and only if* ρ_{AB} *is entangled* [8], we get the upper bound of n-extension of an entangled state ρ_{AB},

$$n \leq N = [\frac{S(\rho_A)}{G_{\leftarrow}(\rho_{AB})}], \qquad (8)$$

where $[x]$ is the maximal integer not larger than x. Thus we proved that for entangled state, there exists a finite number N such that no n-extension can be found for $n > N$. Physically, entanglement in a given state can not be sharable in arbitrarily many parties.

For the system of many identical particles, the state $\rho_{A_1A_2,\cdots,A_n}$ has the symmetry of permutation. It holds for any state that entanglement between any pair particles tends to zero as $n \to \infty$.

In summary, we give a simple proof of monogamy of entanglement and provide an upper bound of the number of parties beyond which entanglement cannot be shared.

Acknowledgement D. Yang would like to thank M. Horodecki for helpful comment.

[1] B. M. Terhal, quant-ph/0307120
[2] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).
[3] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[4] J. Bae and A. Acin, quant-ph/0603078.
[5] M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
[6] L. Henderson and V. Vedral J. Phys. A **34**, 6899 (2001).
[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005).